Remarks

Upon entry of the foregoing amendment, claims 22-25, 27, 28, 47-50, 52, 53 and 57 are pending in the application, with claims 22, 47 and 57 being the independent claims. Claims 1-21, 26, 29-46 and 51 are sought to be cancelled without prejudice to or disclaimer of the subject matter therein. Claims 54-56 had previously been cancelled. New claim 57 is sought to be added. Claims 23-25, 28, 47-50 and 53 are sought to be amended. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Information Disclosure Statement

The Examiner attached to the Office Action copies of the Forms PTO-1449 from the IDS filed on June 25, 2001, and from the IDS filed on September 23, 2002. The Examiner is thanked for reviewing and returning these documents. On the single page Form PTO-1449 from the IDS of June 25, 2001, however, the Examiner did not initial document AA1, indicating consideration of that document. It is respectfully requested that the Examiner initial the Form PTO-1449 in the appropriate space to indicate consideration of document AA1, and that a copy of that form be sent to the undersigned.

Claim Amendments

The amendments sought to be made to claims 23-25, 28, 48-50 and 53 are being made simply to change the dependencies of these claims. Claim 47 is being amended to put the claim in independent format. These amendments are not being made to distinguish the cited art, and are not intended to narrow the scope of the claims in any way.

Rejections under 35 U.S.C. § 102

In the Office Action, the Examiner rejected claims 1-53 under 35 U.S.C. §102(b) as being unpatentable over U.S. Patent No. 5,625,693 to Rohatgi *et al.* (hereafter "Rohatgi"). Applicants respectfully traverse this rejection. The present application is a continuation of International Application No. PCT/EP97/02111, filed April 25, 1997. Rohatgi issued as a U.S. patent on April 29, 1997, AFTER the filing of the present International Application. As a result, Rohatgi does not qualify as prior art under 35 U.S.C. §102(b). This rejection is therefore improper, and its reconsideration and withdrawal is respectfully requested.

Additional Comments

After entry of the present amendment, claims 22-25, 27, 29, 47-50, 52, 53 and 57 are pending in this application. To the extent that the Examiner might apply the Rohatgi-based rejection to these pending claim under 35 U.S.C. §102(e), Applicants provide comments below on why these pending claims are patentable over Rohatgi.

The present invention includes a method of downloading data to an MPEG receiver/decoder. On the transmitting side, a signature for the data to be downloaded is

generated, the signature and other data is included in a block of data with a selected offset between the start of the data block and the start of the signature, the data block is encrypted using a private key, the data to be downloaded and the encrypted data block are then formatted as an MPEG table and transmitted. Then, at the receiver/decoder, the MPEG table is received, and the encrypted data block in the received MPEG table is decrypted using a public key corresponding to the private key. At least one stored offset is looked up in a protected area of memory of the receiver/decoder. The stored offset is used to extract the signature from the decrypted data block. Finally, a signature for the data in the received MPEG table is generated and compared with the signature extracted from the decrypted data block.

Rohatgi teaches an apparatus and method for authenticating applications transmitted over an interactive TV system. An application is divided into a directory module and one or more code modules and data modules, which can be further divided into transmission units. The preferred method of protecting the modules comprises performing hash functions over respective modules, inserting the respective hash values in further security information fields of the directory module and then performing a hash function over the directory module. The hash value of the directory module is then encrypted with the application provider's private encryption key.

One main difference between the present invention and Rohatgi is that, in the present invention, the signature that is generated for the data is included together with other data in a block of data with a selected offset between the start of the data block and the start of the signature. The effect of this offset is to hide the signature in a field of dummy data, effectively making it much harder to find, and thus increasing security.

In contrast, the Module Transmission Unit Byte Offset of Rohatgi does not have the same function or solve the same problem as does the offset in the present invention. Rohatgi needs the offset in order to know where the payload of the Transmission Unit starts, since there are an unknown number of reserved bytes between the offset and the payload. Rohatgi is silent on the use of these reserved bytes, but it is common practice to reserve bytes for, for example, future use (i.e., to make it possible to adapt the headers for future developments). As such, the nature or number of these bytes would be unknown in the present. Rohatgi's offset is thus needed to know where the first byte of the payload data is positioned.

Another main difference is that, in Rohatgi, the offset is transmitted in the Transmission Unit header (see Figure 5). This is not the case in the present invention, where it is looked up in a protected area of memory of the receiver/decoder. Transmitting the offset value with the data (as taught by Rohatgi) does not give the same security advantages as are achieved by the invention.

For at least these reasons, the present invention is distinguishable from the teachings of Rohatgi.

The pending claims clearly recite these steps/features of the invention which define the invention over Rohatgi. For example, independent claim 22 recites, *inter alia*:

> **including the signature and other data in a block of data with a selected offset between the start of the data block and the start of the signature;**
> encrypting the data block using a private key;
> formatting the data to be downloaded and the encrypted data block as an MPEG table;
> transmitting the MPEG table; and
> at the receiver/decoder:
> receiving the MPEG table;
> decrypting the encrypted data block in the received MPEG table using a public key corresponding to the private key;

looking up at least one stored offset in a protected area of memory of the receiver/decoder;

extracting the signature from the decrypted data block using said one looked-up offset from the start of the decrypted data block;

generating a signature for the data in the received MPEG table; and

comparing the signature extracted from the decrypted data block with the signature generated at the receiver/decoder for the received data. [Emphasis added.]

These claimed features are neither taught nor suggested by Rohatgi. Accordingly, claim 22 is patentable over Rohatgi. Reconsideration and allowance of this claims is respectfully solicited.

Similar to claim 22, independent claim 47 recites features concerning use of the offset and storage of the offset in a protected area of memory. Thus, claim 47 is patentable over Rohatgi for at least the same reasons that claim 22 is patentable.

Each of claims 23-25, 27, 29, 47-50, 52 and 53 depends either directly or indirectly from one of independent claims 22 or 47. Thus, these dependent claims are patentable over Rohatgi for at least the same reasons that claim 22 is patentable. Reconsideration and allowance of these dependent claims is respectfully solicited.

New claim 57 is also believed to be patentable over Rohatgi. Consideration and allowance of this new claim is respectfully solicited.

Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for

allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Michael B. Ray
Attorney for Applicants
Registration No. 33,997

Date: 4/6/04

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

MBR/agj
243270_2.DOC